

**MCR TEKSTİL DIŐ TİCARET
LİMİTED ŐİRKETİ
KİŐİSEL VERİLERİ SAKLAMA VE İMHA
POLİTİKASI**

6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNUNA GÖRE

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1.POLİTİKANIN AMACI:

İşbu Kişisel Veri Saklama ve İmha Politikası, 6698 Sayılı Kişisel Verilerin Korunması Kanunu ve buna bağlı olarak düzenlenen Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi Hakkında Yönetmelik uyarınca hukuki yükümlülüklerimizi yerine getirmek ve kişisel veri sahiplerini kişisel verilerinizin işlendikleri amaç için gerekli olan azami saklama süresinin belirlenmesi esasları ile kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi yani imha süreçleri hakkında bilgilendirmek, uygulanacak kurallar ve sorumlulukları belirlemek amacıyla veri sorumlusu sıfatıyla şirketimiz tarafından hazırlanmıştır.

2.POLİTİKANIN KAPSAMI:

İşbu Politika, şirketimizin tüm çalışanları, çalışan adayları, yöneticileri, danışmanları, ziyaretçileri, hizmet sağlayıcıları ve diğer üçüncü kişilere ait kişisel veriler ve bu Politika kapsamında olup şirketin sahip olduğu ya da şirketçe yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde uygulanır.

Politika, Kanun'da belirtildiği şekilde, tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla verilerin işlendiği sistemlerde yer alan kişisel verileri kapsamaktadır

Politika'da aksi belirtilmediği sürece kişisel veriler ve özel nitelikli kişisel veriler birlikte 'Kişisel Veriler' olarak adlandırılacaktır.

İşbu Politika, Mcr Tekstil Dış Ticaret Limited Şirketi tarafından düzenlenmiştir ve mcrgiyim.com internet sitesinde yayınlanır, kişisel veri sahiplerinin talebi üzerine ilgili kişilerin erişimine sunulur.

4.KİŞİSEL VERİ SAKLAMA VE İMHAYA İLİŞKİN İLKELER:

Şirketimiz tarafından kişisel verilerin saklanması ve imhasında aşağıda yer alan temel ilkeler benimsenmiştir:

- 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nda yer alan kişisel verilerin işleme şartlarının tamamı ortadan kalkması durumunda, kişisel veriler şirketimizce resen veya kişisel veri sahibinin talebi üzerine silinmekte, yok edilmekte veya anonim hale getirilmektedir.
- Kişisel Verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi, Kanun'un 4. maddesinde sayılan ilkeler ve 12.maddesi kapsamında alınması gereken teknik ve

idari tedbirler başta olmak üzere, ilgili mevzuat hükümleri, Kurul kararları ve işbu Politika ile uyumlu olarak icra edilmektedir. Bu kapsamda, Kanun'un 4.maddesi uyarınca:

- 1.Hukuka ve dürüstlük kurallarına uygunluk,
- 2.Doğruluk ve gerektiğinde güncellik,
- 3.Belirlilik, açıklık ve meşru amaçlar için işlenme,
- 4.İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,
- 5.İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkeleri Şirketimiz için önceliklidir.

Kanun'un 12.maddesine paralel olarak da, Şirketimiz:

- a. Kişisel Verilerin hukuka aykırı olarak işlenmesini önlemek,
- b. Kişisel Verilere hukuka aykırı olarak erişilmesini önlemek,
- c. Kişisel Verilerin muhafazasını sağlamak,

Amacıyla, uygun güvenlik düzeyini temin etmeye yönelik işbu Politika'da benimsenmiş olan teknik ve idari tedbirleri almaktadır.

- Kişisel verilerin silinmesi, yok edilmesi, anonim hale getirilmesiyle ilgili yapılan tüm işlemler Şirketimiz tarafından kayıt altına alınmakta ve söz konusu kayıtlar, Şirketimizin uyum göstermesi gereken diğer hukuki yükümlülükleri hariç olmak üzere, en az on (10) yıl süreyle saklanmaktadır.
- Kurul tarafından aksine bir karar alınmadıkça, Kişisel Verileri re'sen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanı Şirketimizce seçilmektedir. Ancak, Veri Sahibinin talebi halinde, uygun yöntem gerekçesi açıklanarak seçilecek veya neden seçilemediğine ilişkin olarak Veri Sahibine gerekli geri bildirim yapılacaktır.

6.SAKLAMA VE İMHA SÜREÇLERİNDE YER ALACAK KİŞİLER VE SORUMLULUKLARI:

Şirketimiz içerisinde Kanun, Yönetmelik ve bu Politika ile belirtilen verinin imhasına ilişkin yükümlülüklerin yerine getirilmesinde tüm çalışanlar, danışmanlar, dış hizmet sağlayıcıları ve sair surette şirketimiz nezdinde kişisel veri saklayan ve işleyen herkes bu gerekleri yerine getirmekten sorumludur.

Her iş birimi kendi iş süreçlerinde ürettiği veriyi saklamak ve korumakla yükümlüdür. Ancak üretilen verinin iş biriminin kontrolü ve yetkisi dışında sadece bilgi sistemlerince bulunması durumunda, söz konusu veri bilgi sistemlerinden sorumlu birimler tarafından saklanacaktır.

İş süreçlerini etkileyecek ve veri bütünlüğünün bozulmasına, veri kaybına ve yasal düzenlemelere aykırı sonuçlar doğmasına neden olacak periyodik imhalar, ilgili kişisel verinin türü içinde yer aldığı sistemler ve veri sahibi iş birimi dikkate alınarak ilgili bilgi

sistemleri bölümlerince yapılacaktır. Aşağıda personellerin görev ve sorumluluk alanları düzenlenmiştir:

PERSONEL	GÖREV	SORUMLULUK
Kurumsal İletişim Grup Şirketler Direktörü	Kurumsal İletişim Departmanı- Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Avukat	Hukuk Departmanı- Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
İnsan Kaynakları Müdürü	İnsan Kaynakları Departmanı- Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Bilgi İşlem Müdürü	Bilgi Teknolojileri Departmanı- Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Muhasebe Müdürü	Mali İşler Departmanı- Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
İdari İşler Müdürü	Veri Sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması

		ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Güvenlik Müdürü	İç Yönerge'de yer alan görevi dahilinde Kişisel Veri Politika'sı ve İmha Politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Pazarlama Müdürü	İç Yönerge'de yer alan görevi dahilinde Kişisel Veri Politika'sı ve İmha Politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi

7.KİŞİSEL VERİLERİN SAKLANDIĞI KAYIT ORTAMLARI:

Veri sahiplerine ait kişisel veriler, şirketimiz tarafından veri sorumlusu sıfatıyla aşağıda listelenen ortamlarda başta 6698 Sayılı KVKK hükümleri olmak üzere ilgili mevzuata uygun olarak, uluslararası veri güvenliği prensipleri çerçevesinde hassasiyetle ve güvenli bir şekilde saklanmaktadır:

- **Elektronik Ortamlar:**

- ✓ Sunucular (Etki alanı, yedekleme, e-posta, veri tabanı, web, dosya paylaşım, vb.)
- ✓ Yazılımlar (Ofis yazılımları, portal, VERBİS...)
- ✓ Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, anti virüs vs.)
- ✓ Kişisel bilgisayarlar (Masaüstü, dizüstü)
- ✓ Mobil cihazlar (telefon, tablet vb.), Optik diskler (CD, DVD, vb.)
- ✓ Çıkarılabilir bellekler (USB, Hafıza Kartı vb.)
- ✓ Yazıcı, tarayıcı, fotokopi makinesi
- ✓ Microsoft Programları
- ✓ Görüntü ve ses kayıt cihazları

- **Elektronik Olmayan Ortamlar:**

- ✓ Kâğıt
- ✓ Manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri vb.)
- ✓ Yazılı, basılı, görsel ortamlar

✓ Arşiv ve dolaplar

8. KİŞİSEL VERİLERİN SAKLANMASI VE İMHASINA İLİŞKİN HUKUKİ SEBEP VE AMAÇLAR:

Veri sahiplerine ait kişisel veriler. Şirketimiz tarafından özellikle ticari faaliyetlerin sürdürülebilmesi, hukuki yükümlülüklerin yerine getirilebilmesi, çalışan haklarının ve yan haklarının planlanması ve uygulanması ile müşteri ilişkilerinin yönetilebilmesi amacıyla yukarıda sayılan fiziki veya elektronik ortamlarda güvenli bir biçimde 6698 Sayılı KVK Kanunu ve diğer ilgili mevzuatta belirtilen sınırlar çerçevesinde saklanmaktadır.

a) Saklamayı Gerektiren Sebepler: Şirketimiz insan kaynakları süreçlerini yürütmek, kurumsal iletişimi sağlamak, kurum güvenliğini sağlamak, istatistiksel çalışmalar yapabilmek, imzaladığımız sözleşmeler çerçevesinde iş ve işlemleri ifa edebilmek, ilerde doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğünü yerine getirebilmek, yasal raporlamalar yapmak, kanunda belirtilen yükümlülüklerimizi tamamlamak gibi amaçlarla kişisel verileri saklamaktadır.

- Kişisel verilerin, sözleşmenin kurulması ve ifası ile doğrudan doğruya ilgili olması nedeniyle saklanması,
- Kişisel verilerin bir hakkın tesisi, kullanılması veya korunması amacıyla saklanması,
- Kişisel verilerin temel hak ve özgürlüklere zarar vermemek şartıyla şirketimizin meşru menfaatlerini korumak için zorunlu olması,
- Kişisel verilerin şirketimizin herhangi bir hukuki yükümlülüğünü yerine getirmesi amacıyla saklanması,
- Mevzuatta kişisel verilerin saklanması açıkça öngörülmesi,
- Veri sahiplerinin açık rızasının alınmasını gerektiren saklama faaliyetleri açısından veri sahiplerinin açık rızasının bulunması.

b) İmhayı Gerektiren Sebepler: Yönetmelik uyarınca, aşağıda sayılan hallerde veri sahiplerine ait kişisel veriler, şirketimiz tarafından re'sen yahut talep üzerine silinir, yok edilir veya anonim hale getirilir:

- Kişisel verilerin işlenmesine veya saklanmasına esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- Kişisel verilerin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- Kanun'da belirtilen kişisel verilerin işlenmesini gerektiren şartların ortadan kalkması,
- Kişisel verileri işlemenin sadece açık rıza şartına bağlı olarak gerçekleştiği hallerde, ilgili kişinin rızasını geri alması,

- İlgili kişinin, Kanun'da belirtilen hakları çerçevesinde kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin yaptığı başvurunun veri sorumlusu tarafından kabul edilmesi,
- Veri sorumlusunun, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabın yetersiz bulunması veya Kanun'da öngörülen süre içinde cevap vermemesi hallerinde; Kurul'a şikâyette bulunulması ve bu talebin Kurul tarafından uygun bulunması,
- Kişisel verilerin saklanması gerektiren azami sürenin geçmiş olmasına rağmen, kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması.

9.KİŞİSEL VERİLERİN KORUNMASINA VE İMHA EDİLMESİNE İLİŞKİN ALINAN TEDBİRLER:

Şirketimiz, KVK Kanunu'nun 12. maddesine uygun olarak, işlemekte olduğu kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, verilere hukuka aykırı olarak erişilmesini önlemek ve verilerin muhafazasını sağlamak için uygun güvenlik düzeyini sağlamaya yönelik gerekli teknik ve idari tedbirleri almakta, bu kapsamda gerekli tüm denetimleri yapmaktadır. İşlenen kişisel verilerin teknik ve idari tüm tedbirler alınmış olmasına rağmen, kanuni olmayan yollarla üçüncü kişiler tarafından ele geçirilmesi durumunda, Şirketimizce bu durum mümkün olan en kısa süre içerisinde ilgili birimlere haber verilmektedir. Aşağıda alınan teknik ve idari tedbirler gösterilmektedir:

1-Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.

2-Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.

3-Anahtar yönetimi uygulanmaktadır.

4-Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.

5-Depolanan kişisel verilerin güvenliği sağlanmaktadır.

6-Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.

7-Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.

8-Çalışanlar için yetki matrisi oluşturulmuştur.

9-Erişim logları düzenli olarak tutulmaktadır.

10-Eriřim, bilgi gvenliđi, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmıř ve uygulamaya bařlanmıřtır.

11-Gerektiđinde veri maskeleye nlemi uygulanmaktadır.

12-Gizlilik taahhtnameleri yapılmaktadır.

13-Grev deđiřikliđi olan ya da iřten ayrılan alıřanların bu alandaki yetkileri kaldırılmaktadır.

14-Gncel anti-virs sistemleri kullanılmaktadır.

15-Gvenlik duvarları kullanılmaktadır.

16-İmzalanan szleřmeler veri gvenliđi hkmleri iermektedir.

17-Kâđıt yoluyla aktarılan kiřisel veriler iin ekstra gvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gnderilmektedir.

18-Kiřisel veri gvenliđi politika ve prosedrleri belirlenmiřtir.

19-Kiřisel veri gvenliđi sorunları hızlı bir Őekilde raporlanmaktadır.

20-Kiřisel veri gvenliđinin takibi yapılmaktadır.

21-Kiřisel veri ieren fiziksel ortamlara giriř ıkıřlarla ilgili gerekli gvenlik nlemleri alınmaktadır.

22-Kiřisel veri ieren fiziksel ortamların dıř risklere (yangın, sel vb.) karřı gvenliđi sađlanmaktadır.

23-Kiřisel veri ieren ortamların gvenliđi sađlanmaktadır.

24-Kiřisel veriler mmkn olduđunca azaltılmaktadır.

25-Kiřisel veriler yedeklenmekte ve yedeklenen kiřisel verilerin gvenliđi de sađlanmaktadır.

26-Kullanıcı hesap ynetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.

27-Kurum ii periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.

28-Log kayıtları kullanıcı mdahalesi olmayacak Őekilde tutulmaktadır.

29-Mevcut risk ve tehditler belirlenmiřtir.

30-zel nitelikli kiřisel veri gvenliđine ynelik protokol ve prosedrlere belirlenmiř ve

uygulanmaktadır.

31-Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmektedir.

32-Özel nitelikli kişisel veriler için güvenli şifreleme / kriptografik anahtarlar kullanılmakta ve farklı birimlerce yönetilmektedir.

33-Saldırı tespit ve önleme sistemleri kullanılmaktadır.

34-Sızma testi uygulanmaktadır.

35-Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.

36-Şifreleme yapılmaktadır.

37-Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişiler veriler şifrelenerek aktarılmaktadır.

38- Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır.

39- Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.

40- Veri kaybı önleme yazılımları kullanılmaktadır.

10.İMHA TEKNİKLERİ:

Şirketimiz ilgili kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde resen veya kişisel veri sahibinin talebi üzerine kişisel verileri silebilir veya yok edebilir. Kişisel verilerin silinmesi akabinde ilgili kişiler hiçbir şekilde silinen verilere tekrardan erişilemeyecek ve kullanılmayacaktır. Şirketimiz tarafından kişisel verilerin imha süreçlerinin tanımlanması ve takip edilmesine ilişkin etkin bir veri takip süreci yönetilecektir. Yürütülen süreç sırası ile silinecek verilerin tespit edilmesi, ilgili kişilerin tespiti, kişilerin erişim yöntemlerinin tespiti ve hemen akabinde verilerin silinmesi olacaktır.

Şirketimiz kişisel verileri yok etmek, silmek veya anonim hale getirmek için verilerin kaydedildiği ortama bağlı olarak aşağıda belirtilen yöntemlerin bir veya birkaçını kullanabilir:

- **Kişisel Verilerin Silinmesi:** Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Veri sorumlusu kişisel verilerin silinmesiyle ilgili her türlü teknik ve idari

tedbirleri almakla sorumludur. Şu yöntemler kullanılarak bu işlem gerçekleştirilebilmektedir:

1-Yazılımdan Güvenli olarak Silme: Tamamen veya kısmen otomatik olan yollarla işlenen ve dijital ortamlarda muhafaza edilen veriler silinirken; İlgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilecek biçimde verinin ilgili yazılımdan silinmesine ilişkin yöntemler kullanılır.

Bulut sisteminde ilgili verilerin silme komutu verilerek silinmesi; merkezi sunucuda bulunan dosya veya dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması; veri tabanlarında ilgili satırların veri tabanı komutları ile silinmesi veya taşınabilir medyada yani flash ortamında bulunan verilerin uygun yazılımlar kullanılarak silinmesi bu kapsamda sayılabilecektir.

Ancak, kişisel verilerin silinmesi işlemi, diğer verilere de sistem içerisinde erişilememe ve bu verileri kullanamama sonucunu doğuracak ise, aşağıdaki koşulların sağlanması kaydıyla, kişisel verilerin ilgili kişiyle ilişkilendirilemeyecek duruma getirilerek arşivlenmesi halinde de kişisel veriler silinmiş sayılacaktır:

- Başka herhangi bir kurum, kuruluş veyahut kişinin erişimine kapalı olması,
- Kişisel verilere yalnızca yetkili kişiler tarafından erişilmesini sağlayacak şekilde gerekli her türlü teknik ve idari tedbirlerin alınması.

2-Uzman Tarafından Güvenli Olarak Silme: Bazı durumlarda kendisi adına kişisel verileri silmesi için bir uzman ile anlaşılabilir. Bu durumda, kişisel veriler bu konuda uzman olan kişi tarafından ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilecek biçimde güvenli olarak silinir.

3-Kâğıt Ortamında Bulunan Kişisel Verilerin Karartılması (Miskeleme): Kişisel verilerin amaca yönelik olmayan kullanımını önlemek veya silinmesi talep edilen verileri silmek için ilgili kişisel verilerin fiziksel olarak kesilerek belgeden çıkartılması veya geri döndürülemez ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak görünemeyecek hale getirilmesi, kapatılması yöntemidir.

- **Kişisel Verilerin Yok Edilmesi:** Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Veri sorumlusu, kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür. Kişisel verilerin yok edilmesi yöntemleri şu şekilde sıralanabilir:

1- De-manyetize Etme: Manyetik medyanın yüksek manyetik alanlara maruz kalacağı özel cihazlardan geçirilerek üzerindeki verilerin okunamaz bir biçimde bozulması yöntemidir. Dikkat edilmelidir ki bu yöntemle yok etme başarılı olmaz ise ancak medyanın fiziksel olarak yok edilmesi ile yok etme işlemi tamamlanmış olabilecektir.

2-Fiziksel Yok Etme: Kişisel veriler herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla da işlenebilmektedir. Bu tür veriler yok edilirken kişisel verinin sonradan kullanılamayacak biçimde fiziksel olarak yok edilmesi sistemi

uygulanmaktadır. Kâğıt ve mikro fiş ortamındaki verilerin yok edilmesi de başka bir şekilde yok edilmeleri mümkün olmadığından bu şekilde gerçekleştirilmelidir.

3-Üzerine Yazma: Üzerine yazma yöntemi, özel yazılımlar aracılığı ile manyetik medya ve yeniden yazılabilir optik medya üzerinden en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazılarak eski verinin okunabilmesi ve kurtarılabilmesini imkânsızlaştıran veri yok etme yöntemidir.

Yukarıda sayılan durumlar gerçekleşmesi sırasında Şirketimiz tarafından; KVKK, Yönetmelik ve ilgili diğer mevzuat hükümlerine veri güvenliğinin sağlanması amacıyla tam uyum sağlamak ve gerekli tüm idari ve teknik tedbirleri almaktadır.

- **Kişisel Verilerin Anonim Hale Getirilmesi:** Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Veri sorumlusu, kişisel verilerin anonim hale getirilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri: Değer düzensizliği sağlamayan anonim hale getirme yöntemleri, saklanmakta olan kişisel verilerde bir değişiklik veya ekleme/çıkarma yapılmaksızın; herhangi bir kişisel veri grubunun genelleme, birbiri ile yer değiştirme veya gruptan belirli bir veri veya alt veri grubunun çıkarılması ile uygulanan anonimleştirmeye yöntemleridir.

1-Değişken Çıkartma: Betimleyici nitelikteki verilerin çıkartılması yöntemi ile toplanılan verilerin bir araya getirilmesinden sonra oluşturulan veri setindeki değişkenlerden “yüksek dereceli betimleyici” olanlar çıkarılarak mevcut veri seti anonim hale getirilmektedir.

2- Kayıtları Çıkartma: Kayıttan çıkarma yönteminde veriler arasında tekillik ihtiva eden veri satırı kayıtlar arasından çıkaralar saklanan veriler anonim hale getirilmektedir.

3-Bölgesel Gizleme: Bölgesel gizleme yönteminde ise tek bir verinin çok az görülebilir bir kombinasyon yaratması sebebi ile belirleyici niteliği mevcut ise ilgili verinin gizlenmesi anonimleştirmeyi sağlamaktadır.

4-Alt ve Üst Sınır Kodlama: Alt ve üst sınır kodlaması yöntemi ile önceden tanımlanmış kategorilerin yer aldığı bir veri grubundaki değerlerin belirli bir ölçüt belirlenerek birleştirilmesiyle anonim hale getirilmektedir.

5-Genelleştirme: Veri toplulaştırma yöntemi ile birçok veri toplulaştırılmakta ve kişisel veriler herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmektedir.

6-Global Kodlama: Veri türetme yöntemi ile kişisel verinin içeriğinden daha genel bir içerik oluşturulmakta ve kişisel verinin herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmesi sağlanmaktadır.

Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri: Değer düzensizliği sağlayan anonim hale getirme yöntemlerinde değer düzensizliği sağlamayanların aksine kişisel veri gruplarında bazı verilerin değiştirilmesi ile bozulma yaratmaktadır. Bu yöntemler kullanılırken elde edilmesi beklenen/istenen fayda doğrultusunda sapmaların dikkatli uygulanması gerekecektir. Toplam istatistiklerin bozulmaması sağlanarak veriden beklenen fayda sağlanmaya devam edilebilir.

1-Gürültü Ekleme: Verilere gürültü ekleme yöntemi özellikle sayısal verilerin ağırlıklı olduğu bir veri setinde mevcut verilere belirlenen oranda artı veya eksi yönde birtakım sapmalar eklenerek veriler anonim hale getirilmektedir.

2-Mikro Birleştirme: Mikro birleştirme yönteminde tüm veriler ilk olarak anlamlı bir sıraya dizilerek (büyükten küçüğe gibi) gruplara ayrılıp, grupların ortalaması alınarak elde edilen değer mevcut gruptaki ilgili verilerin yerine yazılarak anonimleştirme sağlanmış olacaktır.

3-Veri Değiş Tokuşu: Veri değiş tokuşu yönteminde saklanan veriler içerisinde seçilen çiftler arasında bir değişkenin değerleri birbiri ile değiştirilir. Genel olarak kategorize edilebilen veriler için kullanılan bu yöntemde amaç veri sahiplerine ait verilerin birbirleri ile değiştirilerek veri tabanının dönüştürülmesidir.

KVKK'nın 28. maddesi uyarınca, kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi durumunda bu durum Kanun kapsamı dışında kalacak ve açık rıza temini gerekmeyecektir.

11.SAKLAMA VE İMHA SÜRELERİ: Şirketimiz, ilgili mevzuatta herhangi bir süre öngörülümüşse bu süre kadar veya kişisel verileri işlendikleri amaç için gerekli olan süre boyunca saklar. Kişisel verilerin esas toplanma amacının veya varsa bu Politikada belirtilen ikincil işleme dayanağının ortadan kalkması halinde kişisel veriler aşağıda belirtilen süreler boyunca saklanmaya devam edilebilir.

Bu sürelerin sona ermesi dolayısıyla silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı durumda Şirketimiz bu tarihi takip eden ilk periyodik imha işleminde kişisel verileri siler, yok eder veya anonim hale getirir.

KİŞİSEL VERİ İÇEREN İŞLEM VEYA SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
Kimlik Bilgisi	40 Yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
İletişim Bilgisi	40 Yıl	Saklama süresinin bitimini takiben 180 gün içerisinde

Lokasyon Bilgisi	40 Yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Özlük Bilgisi	40 Yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Hukuki İşlem Bilgisi	10 Yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Müşteri İşlem	10 Yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Fiziksel Mekân Güvenliği	3 Ay	Saklama süresinin bitimini takiben 180 gün içerisinde
İşlem Güvenliği	3 Yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Risk Yönetimi	10 Yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Finansal Bilgiler	10 Yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Mesleki Deneyim	10 Yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Pazarlama	3 Yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Görsel ve İşitsel Kayıtlar	40 Yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Kılık ve Kıyafet	İşlem Tamamlanıncaya Kadar Geçen Süre Kadar	Saklama süresinin bitimini takiben 180 gün içerisinde
Sağlık Bilgileri	3 Yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Ceza Mahkumiyeti ve Güvenlik Tedbirleri	10 Yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Biyometrik Veri	İşlem Tamamlanıncaya Kadar Geçen Süre Kadar	Saklama süresinin bitimini takiben 180 gün içerisinde

12.PERİYODİK İMHA SÜRESİ:

Şirketimizin periyodik imha süresi 6 aydır. Saklama süresi dolan kişisel veriler, yukarıda belirtilen imha süreleri çerçevesinde, 6 aylık periyodlarla işbu Politika'da yer verilen usullere uygun olarak imha edilir. Söz konusu sistemlerde bilgilerin tekrar geri getirilmeyecek şekilde, verilerin kaydedildiği varsa evrak, dosya, CD, disket, hard disk gibi araçlardan geri dönüştürülmeyecek şekilde silinecektir.

Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanır.

13.KİŞİSEL VERİ SAHİBİNİN BAŞVURUSU VE HAKLARINI KULLANMASI:

İlgili kişi, ilgili mevzuat hükümlerinde yer alan haklarına ilişkin taleplerini kimliklerini tespit edecek bilgi ve belgelerle internet sitemizde bulunan başvuru formunu, bu formda yer alan başvuru yollarından biriyle şirketimize ileterek kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep edebilir. Veri sahibi tarafından yapılacak başvurunun şirketimize ulaşması halinde, şirketimiz;

1-Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa, talebe konu kişisel verileri silmekte, yok etmekte veya anonim hale getirmektedir. Bu surette veri sahibinin talebi en geç otuz (30) gün içerisinde sonuçlandırılmakta ve kendisine bilgi verilmektedir.

2-Kişisel veri işleme şartlarının tamamı ortadan kalkmamışsa, şirketimize yöneltilen talep, söz konusu durum hakkında gerekçeli bilgilendirme yapılarak reddedilmektedir. Bu bilgilendirme ilgili kişiye en geç otuz (30) gün içinde, yazılı olarak veya elektronik ortamda yapılmaktadır. Şirketimiz aşağıdaki gerekçelerle veri sorumlusuna ait kişisel verinin silinmesini reddedebilir:

- Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi.
- Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi.
- Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş

kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbarî faaliyetler kapsamında işlenmesi.

- Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.
- Kişisel veri işleminin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması.
- Kişisel veri sahibi tarafından kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi.
- Kişisel veri işleminin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması.
- Kişisel veri işleminin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması.
- Kişisel veri sahibinin talebinin diğer kişilerin hak ve özgürlüklerini engelleme ihtimali olması
- Orantısız çaba gerektiren taleplerde bulunmuş olması
- Talep edilen bilginin kamuya açık bir bilgi olması.

Kişisel veri sahibi KVK Kanunu'nun 14. maddesi gereğince başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hâllerinde; Şirketimizin cevabını öğrendiği tarihten itibaren otuz ve herhâlde başvuru tarihinden itibaren altmış gün içinde KVK Kurulu'na şikâyetle bulunabilir.

3-Kişisel veri işleme şartlarının tamamı ortadan kalkmış fakat veri sahibinin talebinde konu olan kişisel veriler üçüncü kişilerle paylaşılmış ise, şirketimize yöneltilmiş talep verilerin paylaşıldığı üçüncü kişiye bildirilmekte ve üçüncü kişi tarafından bu Politika ve mevzuat çerçevesinde gerekli işlemlerin yapılması talep edilmektedir.

Şirketimiz, başvuruda bulunan kişinin kişisel veri sahibi olup olmadığını tespit etmek adına ilgili kişiden bilgi talep edebilir. Şirketimiz, kişisel veri sahibinin başvurusunda yer alan hususları netleştirmek adına, kişisel veri sahibine başvurusu ile ilgili soru yöneltebilir.

Kişisel veri sahipleri adına üçüncü kişilerin başvuru talebinde bulunabilmesi için veri sahibi tarafından başvuruda bulunacak kişi adına noter kanalıyla düzenlenmiş özel vekâletname bulunmalıdır.

13.POLİTİKANIN YAYINLANMASI VE SAKLANMASI:

İşbu Politika, basılı kâğıt ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, internet sayfasında kamuya açıklanır. Basılı kâğıt nüshası şirket bünyesinde saklanır.

14.DEĐİŐİKLİK:

Őirketimiz, iŐbu Metin'de yer alan hűkűmleri dilediĐi zaman yayımlamak suretiyle deĐiŐtirebilir. Őirket'in deĐiŐiklik yaptıĐı hűkűmler mcrqiyim.com'da yayımlandıĐı tarihte yűrűrlűk kazanır.